REMARKS

In the Final Office Action dated January 27, 2005, claims 1-10 are pending. Claims 1 and 10 are independent claims from which all other claims depend therefrom. Claims 1 and 10 have been amended. Note that claims 1 and 10 have not been amended for patentability reasons.

Claims 1 and 10 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Preston et al. (U.S. Publication No. 2002/0032853), in view of Willis et al. (U.S. Patent No. 6,385,647).

Claims 1 and 10 have similar limitations and are therefore discussed together. Claim 1 recites a virtual biological fluid system for secure communications. The system includes a primary gateway having security information and multiple communication layers. A security control plane is coupled to and formed using information from each of the communication layers. The control plane in conjunction with the security information forms a virtual biological fluid insuring secure data transmission. Claim 10 recites a method for secure communications over a network. Claim 10 has similar limitations to that of claim 1.

The Office Action states that the claim language of claims 1 and 10 do not specifically mention the security control plane being coupled to each of the layers. Applicants submit that claims 1 and 10 have been amended to recite such limitation, which is not taught or suggested by the prior art. However, Applicants submit that claims 1 and 10 are allowable without such recitation.

As stated in the previous Response, Preston does not teach or suggest the use of a security control plane in conjunction with security information to form a virtual biological fluid. The security managers of Preston use encryption keys for security; see paragraph [0016] and Figures 2A, 2B, and 3 of Preston. The encryption keys are utilized in a single layer, the session layer. The use of an

encryption key, as stated in the background section of the present application, does not protect against eavesdropping and data gathering and post processing. The use of an encryption key also does not allow a system to detect a breach in security and may allow for computation sharing for key acquisition.

In addition, note that the claimed security control plane is both **coupled to** and **formed** using information from each of the communication layers. The security managers of Preston are not formed from information received from each of the communication layers. The security managers are software entities that pre-exist as part of the system of Preston and are used to generate and decode encryption keys. Also, there is no inference or disclosure of such formation in Preston. Although the encryption keys are passed between layers the security managers do not utilize information from each layer to form a security plane. Passing messages through communication layers to a security manager is clearly different than forming a security plane through information received from each of the layers.

Furthermore, the security managers of Preston do not act as security planes through use of information from each of the communication layers. The security managers rather generate and decode encryption keys, which the security managers transmit through and receive from multiple communication layers.

Moreover, Preston fails to disclose the use of a security control plane in conjunction with a station containing security information to form a virtual biological fluid. The formation of a virtual biological fluid enables the use of an interactive security doctrine that allows for multiple levels of security deployment. Preston does not teach or suggest such formation and fails to disclose multiple levels of security deployment.

The security technique of Preston may be referred to as an individual security protocol through the use of encryption keys. The security of Preston

occurs at the session layer only and the topology of the Preston system is fixed and known. The claimed invention allows for the integration of information from all layers of communication into a security plane for improved protection and the topology is variable and unknown.

Applicants submit that since Willis, like Preston, does not teach or suggest a security control plane formed using information from multiple communication layers or the use of a security control plane in conjunction with security information to form a virtual biological fluid, that Preston and Willis alone or in combination fail to teach or suggest each and every limitation of claims 1 and 10. Thus, claims 1 and 10 are novel, nonobvious, and are in a condition for allowance.

Also, as sated in the previous Response, Referring to MPEP § 2143.01, the fact that references can be combined or modified is not sufficient to establish *Prima Facie* obviousness. The prior art must also suggest the desirability of the combination and the modification, *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). None of the references suggest such combination and clearly none of the references suggest performing some sort of combination and modification thereof to arrive at the system and method of claims 1 and 10.

Applicants have also provided arguments submitting that Willis is nonanalogous art. Applicants submit that these arguments are valid and are restated below. Referring to MPEP 2141.01(a), while the Patent Office classification of references and cross-references in the official search notes are some evidence of "nonanalogy" or "analogy" respectively, the court has found "the similarities and differences in structure and function of the inventions to carry far greater weight." *In re Ellis*, 476 F.2d 1370, 1372, 177USPQ526, 527 (CCPA 1973). Willis would not have logically commended itself to an inventor's attention in considering the problems solved by the system and method of claims 1 and 10. In developing a satellite system for secured communication, one would

clearly not look to a method for selectively routing data based on the size of the data. Willis is directed to the efficiency of data communication not the security thereof. Although Willis mentions that a secure transfer protocol may be used, Willis does not describe the operation, functioning, or configuration of a security system. The system of Willis would not have logically commended itself to the Applicant's attention in solving the problems associated with secure communication. Willis would not be reasonably pertinent to the particular problems solved by the system and method of claims 1 and 10. Thus, the Applicant submits that Willis is nonanalogous art.

Applicant submits that since the rejections with respect to claims 1 and 10 have been overcome that claims 1 and 10 are novel, nonobvious, and are in a condition for allowance.

Claims 2-9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Preston and Willis in view of Greene (U.S. Patent No. 6,578,145).

Applicant submits that since claims 2-9 depend from claim 1, claims 2-9 are novel, nonobvious, and are in a condition for allowance for at least the same reasons as put forth above with respect to claim 1. In addition, Greene, like Preston and Willis, also fails to teach or suggest a security control plane that is both coupled to and formed using information from each of multiple communication layers and the use of a control plane in conjunction with security information to form a virtual biological fluid for secure data transmission.

In light of the amendments and remarks, Applicant submits that all rejections are now overcome. The Applicant has added no new matter to the application by these amendments. The application is now in condition for allowance and expeditious notice thereof is earnestly solicited. Should the Examiner have any questions or comments, he is respectfully requested to call the undersigned attorney.

Respectfully submitted,

Georgann S. Grunebach
Registration No. 33,179
Attorney for Applicant

Date: March 15, 2005

The DIRECTV Group, Inc.
RE / R11 / A109
2250 East Imperial Highway
P.O. Box 956
El Segundo, CA 90245
Telephone: (310) 964-4615